E-LEGITIMATIONS NÄMNDEN

Entity Categories for the Swedish eID Framework

ELN-0606-v1.5
Version 1.5
2016-11-16

www.elegnamnden.se

Postadress	Besöksadress	Telefon växel	E-postadress
171 94 SOLNA	**Korta gatan 10**	**010-574 21 00**	**kansliet@elegnamnden.se**

1 Introduction

This specification contains the Entity Category definitions that are defined for the Swedish eID Framework and that should be supported by Service Providers and Identity Providers that are part of the federation.

The use of Entity Categories for the Swedish eID Framework is restricted to SAML metadata where Entity Categories are placed as SAML attributes under the `<mdattr:EntityAttributes>` element ([SAML2MetaAttr]) for an `<md:Extensions>` element ([SAML2Meta]).

```
<md:EntityDescriptor entityID="https://eid2.example.com/entityid">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      ...
      <saml:Attribute Name="http://macedir.org/entity-category"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xsi:type="xs:string">http://id.elegnamnden.se/ec/1.0/loa3-pnr</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
```

*The Entity Category identifier **http://id.elegnamnden.se/ec/1.0/loa3-pnr** specified as an entity attribute for a Service Provider or Identity Provider.*

Three types of Entity Categories are used within the federation:

- Service entity category – Identifiers for entity categories representing alternative sets of requirements.
- Service property categories – Identifiers for defined service properties.
- Service type categories – Identifiers for defined service types.

1.1 Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to technically interoperate without additional negotiation, and should be undertaken with caution.

1.2 References to SAML 2.0 Standards and Profiles

When referring to elements from the SAML 2.0 core specification [SAML2Core], the following syntax is used:

- `<saml2p:Element>` – for elements from the SAML 2.0 Protocol namespace.
- `<saml2:Element>` – for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specifications, the following syntax is used:

- `<md:Element>` – for elements defined in [SAML2Meta].
- `<mdattr:Element>` – for elements defined in [SAML2MetaAttr].

1.3 Consuming and Providing Services

Entity categories are mainly used for service matching. This allows matching of a consuming service with an appropriate providing service. A consuming service in this context is an assertion or attribute consuming service of a service provider (Service described through an `<md:SPSSODescriptor>` element in the federation metadata). A providing service in this context is a service, represented in the federation metadata, providing assertions to a service provider.

The entity categories defined in this document have different meaning depending on whether they are declared by a consuming or a providing service. Further, different types of entity category identifiers defined in this document have different matching rules to determine whether particular providing service matches the requirements of a consuming service.

These differences are outlined in the following table:

EC type	Consuming service	Providing service	Service matching rule
Service Entity Category	Each declared category represents an alternative set of requirements for the service.	Represents the ability to deliver assertions in accordance with each declared category.	At least one of the entity categories declared by the consuming service MUST be declared by the providing service.
Service Property	Represents a property of this service.	Represents the ability to deliver assertions to a consuming service that has the declared property.	All properties declared by the consuming service MUST be declared by the providing service.
Service Type	Declares the type of service provided by this consuming service.	Not applicable.	No matching rule.

1.4 Use in Discovery

Entity Categories in metadata are declarations of requirements and capabilities of Service Providers and Identity Providers. A discovery process may make use of these declared Entity Categories when performing filtering, i.e., when deciding which Identity Providers to present for the end-user. The filtering algorithm is very simple:

> For a Service Provider requesting discovery its metadata entry is scanned for Entity Category identifiers of the type Service Entity Category and Service Property. The algorithm then iterates over all Identity Providers found in the metadata repository for the federation. The discovery process SHOULD display Identity Providers as a plausible choice, if and only if, they have declared;
>
> - at least one of the Service Entity Category identifiers declared by the Service Provider, and
> - all of the Service Property identifiers declared by the Service Provider.

1.5 Representation of Entity Categories in Metadata

Entity categories defined in this document are placed in an entity's metadata record as an attribute value within an entity category attribute (SAML attribute with name `http://macedir.org/entity-category`). If more than one entity category identifier is included in the metadata of a service, it MUST be placed as multiple attribute values within a single entity category attribute.

```
<md:EntityDescriptor entityID="https://eid2.example.com/entityid">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      ...
      <saml:Attribute Name="http://macedir.org/entity-category"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">http://id.elegnamnden.se/ec/1.0/loa3-pnr</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">http://id.elegnamnden.se/sprop/1.0/mobile-auth</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
```

Example of how entity categories are represented in metadata.

2 Definitions for Service Entity Categories

This section contains a listing of all Service Entity Categories that are defined within the framework for Swedish eID.

Service entity category requirements are typically a combination of, but not limited to, the following types of requirements:

- Level of assurance (LoA) attributes as specified in [EidRegistry].
  - Indicating that only services conforming to at least the specified level of assurance have the capability to satisfy the security requirements of the Service Provider. An Identity Provider declaring this Service Entity Category MUST be able to provide this level of assurance.
- Attributes as specified in [EidAttributes].
  - Indicating that only services that implement attribute release according to the identified attribute set have the capability to satisfy the minimum attribute requirements of the Service Provider. An Identity Provider declaring this Service Entity Category MUST be able to provide these attributes.

All Assertion Requirements identifiers are prefixed with "**http://id.elegnamnden.se/ec**".

Note: The main purpose of Service Entity Categories is for service matching before sending a request to a service in order to prevent requests from being sent to a service that will not be able to send a useful response (see section 1.4 above). The technical obligation of the providing service is limited to provide services according to its own declared service entity category regardless of which service entity category that has been declared by the requesting service. The providing service MAY or MAY NOT need to inspect the service entity category of the requesting service to determine how to provide a service once a request is received.

Service Providers MAY also override certain requirements in specific requests. For example, a Service Provider declaring a Service Entity Category that indicates that it will request authentication according to level of assurance 3, MAY still send an authentication request specifying another level of assurance. Any legal or other regulatory obligations that influences this matter is outside the scope of this docu-

ment. One such obligation could be that release of certain sensitive attributes MUST NOT be done unless the Service Provider has declared a particular service entity category.

2.1 loa3-pnr

URL	http://id.elegnamnden.se/ec/1.0/loa3-pnr
Description	User authentication according to assurance level 3 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).
LoA-identifier	http://id.elegnamnden.se/loa/1.0/loa3
Attribute requirements	ELN-AP-Pnr-01 (http://id.elegnamnden.se/ap/1.0/pnr-01) Natural Personal Identity with Civic Registration Number (personnummer)
Other	No additional requirements.

2.2 loa2-pnr

URL	http://id.elegnamnden.se/ec/1.0/loa2-pnr
Description	User authentication according to assurance level 2 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).
LoA-identifier	http://id.elegnamnden.se/loa/1.0/loa2
Attribute requirements	ELN-AP-Pnr-01 (http://id.elegnamnden.se/ap/1.0/pnr-01) Natural Personal Identity with Civic Registration Number (personnummer)
Other	No additional requirements.

2.3 loa4-pnr

URL	http://id.elegnamnden.se/ec/1.0/loa4-pnr
Description	User authentication according to assurance level 4 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).
LoA-identifier	http://id.elegnamnden.se/loa/1.0/loa4
Attribute requirements	ELN-AP-Pnr-01 (http://id.elegnamnden.se/ap/1.0/pnr-01) Natural Personal Identity with Civic Registration Number (personnummer)
Other	No additional requirements.

2.4 eidas-naturalperson

URL	http://id.elegnamnden.se/ec/1.0/eidas-naturalperson
Description	User authentication according to any of the eIDAS assurance levels and attribute release according to “eIDAS Natural Person Attribute Set” (ELN-AP-eIDAS-NatPer-01).
LoA-identifier	Not applicable
Attribute	ELN-AP-eIDAS-NatPer-01 (http://id.elegnamnden.se/ap/1.0/eidas-natural-person-01)

requirements

Other No additional requirements.

It does not make sense to specify the level of assurance for a Service Entity Categories intended for eIDAS since this information is not known to the Swedish eIDAS-node.

3 Definitions for Service Property Categories

A Service Property Entity Category identifier is specified as an attribute value in the entity category attribute in the federation metadata and has the purpose of representing a particular service property.

All Service Type identifiers are prefixed with "**http://id.elegnamnden.se/sprop**".

3.1 mobile-auth

URL	http://id.elegnamnden.se/sprop/1.0/mobile-auth
Description	A service property declaring that the service is adapted to mobile clients and MUST allow users to authenticate using a mobile device that is used to access such service.

For a providing service, i.e. an Identity Provider, inclusion of the mobile-auth category states that the Identity Provider supports authentication using mobile devices, **and** that the end-user interface of the Identity Provider is adapted for mobile clients.

Note that an Identity Provider may of course support authentication for both desktop and mobile users. In these cases the service must be able to display end user interfaces for both types of clients.

A discovery process will use this Service Property when performing filtering of possible Identity Providers, as described in 1.4, "Use in Discovery". This means that a consuming service may include the mobile-auth category in its metadata in order to have the discovery process especially displaying Identity Providers that offer authentication using mobile devices.

See [EidDiscovery] for a more extensive explanation of the use of the mobile-auth category.

4 Definitions for Service Type Entity Categories

A Service Type Entity Category identifier is specified as an entity attribute in the federation metadata and has the purpose of representing a particular service type.

All Service Type identifiers are prefixed with "**http://id.elegnamnden.se/st**".

4.1 sigservice

URL	http://id.elegnamnden.se/st/1.0/sigservice
Description	A service type for a Service Provider that provides electronic signature services within the Swedish eID framework.

5 References

[RFC2119]
Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[SAML2Core]
OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2Meta]
OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2MetaAttr]
OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009.

[EntCat]
The Entity Category SAML Entity Metadata Attribute Type, March 2012.

[EidTillit]
Tillitsramverk för Svensk E-legitimation.

[EidRegistry]
Registry for identifiers assigned by the Swedish e-identification board.

[EidAttributes]
Attribute Specification for the Swedish eID Framework.

6 Changes between versions

Changes between version 1.4 and version 1.5:

- Introduced the Service Entity Category “eidas-naturalperson” (section 2.4) for support of authentication against the eIDAS Framework.
- Minor changes regarding discovery.

Changes between version 1.3 and version 1.4:

- Version 1.3 of [Eid2Attributes] changed the terms “attribute profiles” to “attribute sets”. This specification has therefore been updated to reflect these changes.
- Chapter 1.5, “Representation of Entity Categories in Metadata”, was added to illustrate how entity categories are represented in metadata.
- Clarifications regarding the definition of Service Entity Categories were made to chapter 2.

Changes between version 1.2 and version 1.3:

- In chapter 1.4, “Use in Discovery Services”, the text that referred to the Discovery Service usage of Service Property Entity Categories when rendering user interfaces was removed.
- In chapter 3.1, “mobile-auth”, changes were made to reflect that the use of mobile-auth no longer governs which type of end user interface the Discovery Service should render.
- In chapter 2, “Definitions for Service Entity Categories”, URIs for attribute profiles were added in definitions of the service entity categories.

Changes between version 1.1 and version 1.2:

- In chapter 2, “Definitions for Service Entity Categories”, two new service entity categories have been defined, loa2-pnr and loa4-pnr.

Changes between version 1.0 and version 1.1:

- The service property category mobile-auth was added.
- Changes was made to chapter 1.4, “Use in Discovery Services”, where mobile-auth was referred.